UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/988,106	11/19/2001	Naoyuki Oe	2985.1000	8073

5514 7590 05/23/2008

FITZPATRICK CELLA HARPER & SCINTO
30 ROCKEFELLER PLAZA
NEW YORK, NY 10112

EXAMINER	
GILLIS, BRIAN J	

ART UNIT	PAPER NUMBER
2141	

MAIL DATE	DELIVERY MODE
05/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/988,106	OE ET AL.	
	Examiner	Art Unit	
	Brian J. Gillis	2141	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 January 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3,6-10,12,15-19,21,24-27,30-34,36-41 and 57-59* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3,6-10,12,15-19,21,24-27,30-34,36-41 and 57-59* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 November 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 1, 3, 6, 10, 12, 15, 19, 21, 24, 31-34, 36-41, and 57-59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hunnicutt et al (US Patent #5,889,952) in view of Hipp (US Patent #6,848,106) in view of Klots et al (US Patent #6,920,475) in view of Phillips et al (US Patent #7,136,903).

Claims 1, 10, and 19 disclose an information processing method, apparatus, and storage medium of controlling access to computer resources managed by an operating system in a computer, the method, apparatus, and storage medium being implemented by a specific resource management program located between the operating system and

an application, comprising: a storing step of storing a management table in a storage medium, wherein the management table provides, for each computer resource managed by the operating system, access right information representing access rights for outputting each computer resource to another computer resource, and conditions under which the access right is validated; an interception step of intercepting an operation request for a first computer resource from a process, before the operation request is transferred to the operating system, and if the process holds the first computer resource, registering a correspondence between the process and the first computer resource in a storage medium resulting in a registered process and a registered computer resource; a determination step of: monitoring a series of operation requests associated with the registered process and the registered computer resource to recognize when the series of operation requests, considered together, has the effect of outputting the registered computer resource to a second computer resource, retrieving from the management table access right information of the registered computer resource and access right information of the second computer resource and, determining whether the registered process has an access right for outputting the registered computer resource to the second computer resource based on the access right information retrieved from the management table; a processing step of, if it is determined in the determination step that the registered process has the access right for outputting the registered computer resource to the second computer resource, transferring the operation request to the operating system and returning a result from the operating system to the registered process; and a denial step of denying the

operation request, if it is determined in the determination step that the registered process does not have the access right for outputting the registered computer resource to the second computer resource. Hunnicutt et al teaches an access control list, which can be associated to a single file, or a list of files, which contains information on which users have access and what types of rights are allowed to the specific user (column 4, lines 44-49, column 5, lines 15-19, figure 3), an access cache which keeps track of access to resources (column 5, lines 27-37), retrieving access information from a table (column 1, lines 54-59), a check system which compares the access rights based on the information retrieved (column 1, lines 54-59 column 5, lines 54-67), and since the request has access to the resource the resource is outputted (column 5, lines 54-67), if a matching access permission exists then access to the file is granted (column 5, lines 58-61), and if no permission is granted an error message is generated to the user denying access (figure 5). It fails to teach intercepting an operation request for a first computer resource from a process, before the operation request is transferred to the operating system, and if the process holds the first computer resource, registering a correspondence between the process and the first computer resource in a storage medium resulting in a registered process and a registered computer resource and monitoring a series of operation requests associated with the registered process and the registered computer resource to recognize when the series of operation requests, considered together, has the effect of outputting the registered computer resource to a second computer resource. Hipp teaches the interception program is between the operating system and the application (Figure 3, column 3, line 59 – column 4, line 21).

Hunnicutt et al and Hipp are analogous art because they are both related to controlling access to computer resources.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the scanning process in Hipp with the system in Hunnicutt et al because costly overhead is prevented and performance is improved (Hipp, column 1, lines 52-63).

Hunnicutt et al in view of Hipp teaches the limitations as recited above. It fails to teach if the process holds the first computer resource, registering a correspondence between the process and the first computer resource in a storage medium resulting in a registered process and a registered computer resource and monitoring a series of operation requests associated with the registered process and the registered computer resource to recognize when the series of operation requests, considered together, has the effect of outputting the registered computer resource to a second computer resource. Klots et al teaches a director keeps track of which resource is handling a request from a process (figure 5, column 6, lines 12-40).

Hunnicutt et al in view of Hipp and Klots et al are analogous art because they are both related to controlling computer resources.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the director in Klots et al with the system in Hunnicutt et al in view of Hipp because fewer system resources are required to manage the system architecture (Klots, column 4, lines 21-25).

Hunnicutt et al in view of Hipp in view of Klots et al teaches the limitations as recited above. It fails to teach monitoring a series of operation requests associated with the registered process and the registered computer resource to recognize when the series of operation requests, considered together, has the effect of outputting the registered computer resource to a second computer resource. Phillips et al teaches monitoring and determining if a request message is able to access a requested file, it is widely known in the art a request may be made in various ways (column 27, lines 39-57).

Hunnicutt et al in view of Hipp in view of Klots et al and Phillips et al are analogous art because they are both related to controlling computer resources.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the monitoring feature in Phillips et al with the system in Hunnicutt et al in view of Hipp in view of Klots et al because maintaining data integrity is provided (Phillips, column 5, lines 56-59).

Claims 3 and 12 disclose the method and apparatus according to claim 1, wherein the access right information designates an access right that is extended but not defined in an existing environment. Hunnicutt et al further teaches using access control lists for different levels of control on the server (column 5, lines 8-25).

Claim 21 discloses the storage medium according to claim 19, wherein the determination step, includes determining whether the access right is present by looking up an access right management table containing resource designation information that designates a specific computer resource, condition information under which the access

right is validated, and access right information that designates an access right that is extended but not defined in an existing environment. Hunnicutt et al further teaches an access control list, which can be associated to a single file, or a list of files. The list contains which users have access and what types of rights are allowed to the specific user (column 4, lines 44-49, column 5, lines 8-25, and figure 3).

Claims 6, 15, and 24 disclose the method, apparatus, and storage medium according to claims 3, 12, and 21, wherein the access right information contains information that designates at least one of a right to move to another medium, a right to copy to another medium, a right to print, a right to write to a shared memory, a right to capture a screen, and a right to restrict use processes. Hunnicutt et al further teaches an access control list, which each file object has associated with it. The list contains access control entries, which defines what type of access the user has, one option is full control, which allows manipulation in any way possible (column 4, lines 63-67).

Claim 31 discloses the medium according to claim 19, wherein the computer resource includes contents of a Web cast, digital broadcasting, and music distribution. Hunnicutt et al further teaches the resources being on a file level which means each file object stored on a server (column 4, lines 44-49, 56-57).

Claims 32, 33, and 34 disclose a system, control method, and storage medium for an information processing system constituted by connecting first and second terminals through a communication network the first and the second terminals being controlled by a specific resource management program located between and operating system and an application for each terminal, comprising: a storing step of storing a

management table in a storage medium, wherein the management table provides, for each computer resource managed by an operating system of the second terminal, access right information representing access rights for outputting each computer resource to another computer resource, and conditions under which the access right is validated; an interception step of intercepting, an operation request for a first computer resource of the second terminal from a process in the first terminal, before the computer resource of the second terminal is accessed via an operating system of the first terminal, and if the process holds the first computer resource, registering a correspondence between the process and the first computer resource in a storage medium resulting in a registered process and a registered computer resource; a determination step of: monitoring a series of operation requests associated with the registered process and the registered computer resource to recognize when the series of operation requests, considered together, has the effect of outputting the registered computer resource to a second computer resource, retrieving from the management table access right information of the registered computer resource and access right information of the second computer resource, and determining whether the registered process has an access right for outputting the registered computer resource to the second computer resource based on the access right information retrieved from the management table; a processing step of, if it is determined in the determination step that the registered process has the access right for outputting the registered computer resource to the second computer resource, transferring the operation request to the operating system in the first terminal and returning a result from the operating system to

the registered process in the first terminal; and a denial step of denying the operation request if it is determined in the determination step that the registered process does not have the access right for outputting the registered computer resource to the second computer resource. Hunnicutt et al teaches an access control list, which can be associated to a single file, or a list of files, which contains information on which users have access and what types of rights are allowed to the specific user (column 4, lines 44-49, column 5, lines 15-19, figure 3), an access cache which keeps track of access to resources (column 5, lines 27-37), retrieving access information from a table (column 1, lines 54-59), a check system which compares the access rights based on the information retrieved (column 1, lines 54-59 column 5, lines 54-67), and since the request has access to the resource the resource is outputted (column 5, lines 54-67), if a matching access permission exists then access to the file is granted (column 5, lines 58-61), and if no permission is granted an error message is generated to the user denying access (figure 5). It fails to teach intercepting an operation request for a first computer resource of the second terminal from a process in the first terminal, before the computer resource of the second terminal is accessed via an operating system of the first terminal, and if the process holds the first computer resource, registering a correspondence between the process and the first computer resource in a storage medium resulting in a registered process and a registered computer resource and monitoring a series of operation requests associated with the registered process and the registered computer resource to recognize when the series of operation requests, considered together, has the effect of outputting the registered computer resource to a

second computer resource. Hipp teaches the interception program is between the operating system and the application (Figure 3, column 3, line 59 – column 4, line 21).

Hunnicutt et al and Hipp are analogous art because they are both related to controlling access to computer resources.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the scanning process in Hipp with the system in Hunnicutt et al because costly overhead is prevented and performance is improved (Hipp, column 1, lines 52-63).

Hunnicutt et al in view of Hipp teaches the limitations as recited above. It fails to teach if the process holds the first computer resource, registering a correspondence between the process and the first computer resource in a storage medium resulting in a registered process and a registered computer resource and monitoring a series of operation requests associated with the registered process and the registered computer resource to recognize when the series of operation requests, considered together, has the effect of outputting the registered computer resource to a second computer resource. Klots et al teaches a director keeps track of which resource is handling a request from a process (figure 5, column 6, lines 12-40).

Hunnicutt et al in view of Hipp and Klots et al are analogous art because they are both related to controlling computer resources.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the director in Klots et al with the system in Hunnicutt et al in view

of Hipp because fewer system resources are required to manage the system architecture (Klots, column 4, lines 21-25).

Hunnicutt et al in view of Hipp in view of Klots et al teaches the limitations as recited above. It fails to teach monitoring a series of operation requests associated with the registered process and the registered computer resource to recognize when the series of operation requests, considered together, has the effect of outputting the registered computer resource to a second computer resource. Phillips et al teaches monitoring and determining if a request message is able to access a requested file, it is widely known in the art a request may be made in various ways (column 27, lines 39-57).

Hunnicutt et al in view of Hipp in view of Klots et al and Phillips et al are analogous art because they are both related to controlling computer resources.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the monitoring feature in Phillips et al with the system in Hunnicutt et al in view of Hipp in view of Klots et al because maintaining data integrity is provided (Phillips, column 5, lines 56-59).

Claims 36, 38, and 40 disclose an apparatus, method, and storage medium connected to a terminal through a communication network, the information processing apparatus and the terminal being controlled by a specific resource management program located between an operating system and an application for each of the information processing apparatus and the terminal, comprising: an interception step of intercepting, an operation request for a first computer resource of the terminal from a

process, before the computer resource of the terminal is accessed via an operating system of the information processing apparatus, and if the process holds the first computer resource, registering a correspondence between the process and the first computer resource in a storage medium resulting in a registered process and a registered computer resource, and a transmitting step of transmitting the operation request intercepted in the interception step to the terminal; a receiving step of receiving a reply to the operation request from the terminal, wherein the terminal: monitors a series of operation requests associated with the registered process and the registered computer resource to recognize when the series of operation requests, considered together, has the effect of outputting the registered computer resource of the terminal to a second computer resource, retrieves from a management table access right information of the registered computer resource and access right information of the second computer resource, and determines whether the registered process has an access right for outputting the registered computer resource to the second computer resource based on the access right information retrieved from the management table, wherein the management table provides, for each computer resource managed by the operating system of the terminal, access right information representing access rights for outputting each computer resource to another computer resource, and conditions under which the access right is validated, wherein in the receiving step a determination result determined by the terminal is received as the reply. Hunnicutt et al teaches the server communicating with other servers and clients using a standard communications protocol (column 3, lines 37-39, figure 1), an access control list, which can be associated to a

single file, or a list of files, which contains information on which users have access and what types of rights are allowed to the specific user (column 4, lines 44-49, column 5, lines 15-19, figure 3), an access cache which keeps track of access to resources (column 5, lines 27-37), retrieving access information from a table (column 1, lines 54-59), a check system which compares the access rights based on the information retrieved (column 1, lines 54-59 column 5, lines 54-67), and since the request has access to the resource the resource is outputted (column 5, lines 54-67), if a matching access permission exists then access to the file is granted (column 5, lines 58-61), and if no permission is granted an error message is generated to the user denying access (figure 5). It fails to teach intercepting an operation request for a first computer resource of the terminal from a process, before the computer resource of the terminal is accessed via an operating system of the information processing apparatus, and if the process holds the first computer resource, registering a correspondence between the process and the first computer resource in a storage medium resulting in a registered process and a registered computer resource and monitoring a series of operation requests associated with the registered process and the registered computer resource to recognize when the series of operation requests, considered together, has the effect of outputting the registered computer resource to a second computer resource. Hipp teaches the interception program is between the operating system and the application (Figure 3, column 3, line 59 – column 4, line 21).

Hunnicutt et al and Hipp are analogous art because they are both related to controlling access to computer resources.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the scanning process in Hipp with the system in Hunnicutt et al because costly overhead is prevented and performance is improved (Hipp, column 1, lines 52-63).

Hunnicutt et al in view of Hipp teaches the limitations as recited above. It fails to teach if the process holds the first computer resource, registering a correspondence between the process and the first computer resource in a storage medium resulting in a registered process and a registered computer resource and monitoring a series of operation requests associated with the registered process and the registered computer resource to recognize when the series of operation requests, considered together, has the effect of outputting the registered computer resource to a second computer resource. Klots et al teaches a director keeps track of which resource is handling a request from a process (figure 5, column 6, lines 12-40).

Hunnicutt et al in view of Hipp and Klots et al are analogous art because they are both related to controlling computer resources.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the director in Klots et al with the system in Hunnicutt et al in view of Hipp because fewer system resources are required to manage the system architecture (Klots, column 4, lines 21-25).

Hunnicutt et al in view of Hipp in view of Klots et al teaches the limitations as recited above. It fails to teach monitoring a series of operation requests associated with the registered process and the registered computer resource to recognize when the

series of operation requests, considered together, has the effect of outputting the registered computer resource to a second computer resource. Phillips et al teaches monitoring and determining if a request message is able to access a requested file, it is widely known in the art a request may be made in various ways (column 27, lines 39-57).

Hunnicutt et al in view of Hipp in view of Klots et al and Phillips et al are analogous art because they are both related to controlling computer resources.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the monitoring feature in Phillips et al with the system in Hunnicutt et al in view of Hipp in view of Klots et al because maintaining data integrity is provided (Phillips, column 5, lines 56-59).

Claims 37, 39, and 41 disclose an apparatus, method, and storage medium connected to a terminal through a communication network, the information processing apparatus and the terminal being controlled by a specific resource management program located between an operating system and an application for each of the information processing apparatus and the terminal, comprising: a storing step of storing a management table in a storage medium, wherein the management table provides, for each computer resource managed by an operating system of the information processing apparatus, access right information representing access rights for outputting each computer resource to another computer resource, and conditions under which the access right is validated; a receiving step of receiving an operation request for a first computer resource of the information processing apparatus from a process of the

terminal, intercepted by the terminal, before the computer resource of the information processing apparatus is accessed via an operating system of the information processing apparatus, and if the process holds the first computer resource, registering a correspondence between the process and the first computer resource in a storage medium resulting in a registered process and a registered computer resource; a determination step of: monitoring a series of operation requests associated with the registered process and the registered computer resource to recognize when the series of operation requests, considered together has the effect of outputting the registered computer resource to a second computer resource, retrieving from the management table access right information of the registered computer resource and access right information of the second computer resource, and determining whether the registered process has an access right for outputting the registered computer resource to the second computer resource based on the access right information retrieved from the management table; a processing step of, if it is determined in the determination step that the registered process has the access right for outputting the registered computer resource to the second computer resource, transferring the operation request to the operating system in the terminal and returning a result to a process in the terminal; and a denial step of denying the operation request if it is determined in the determination step that the registered process does not had the access right for outputting the registered computer resource to the second computer resource. Hunnicutt et al teaches a server communicating with other servers and clients using a standard communications protocol (column 3, lines 37-39, figure 1), an access control list, which

can be associated to a single file, or a list of files, which contains information on which users have access and what types of rights are allowed to the specific user (column 4, lines 44-49, column 5, lines 15-19, figure 3), an access cache which keeps track of access to resources (column 5, lines 27-37), retrieving access information from a table (column 1, lines 54-59), a check system which compares the access rights based on the information retrieved (column 1, lines 54-59 column 5, lines 54-67), and since the request has access to the resource the resource is outputted (column 5, lines 54-67), if a matching access permission exists then access to the file is granted (column 5, lines 58-61), and if no permission is granted an error message is generated to the user denying access (figure 5). It fails to teach receiving an operation request for a first computer resource of the information processing apparatus from a process of the terminal, intercepted by the terminal, before the computer resource of the information processing apparatus is accessed via an operating system of the information processing apparatus, and if the process hold the first computer resource, registering a correspondence between the process and the first computer resource in a storage medium resulting in a registered process and a registered computer resource and monitoring a series of operation requests associated with the registered process and the registered computer resource to recognize when the series of operation requests, considered together, has the effect of outputting the registered computer resource to a second computer resource. Hipp teaches the interception program is between the operating system and the application (Figure 3, column 3, line 59 – column 4, line 21).

Hunnicutt et al and Hipp are analogous art because they are both related to controlling access to computer resources.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the scanning process in Hipp with the system in Hunnicutt et al because costly overhead is prevented and performance is improved (Hipp, column 1, lines 52-63).

Hunnicutt et al in view of Hipp teaches the limitations as recited above. It fails to teach if the process holds the first computer resource, registering a correspondence between the process and the first computer resource in a storage medium resulting in a registered process and a registered computer resource and monitoring a series of operation requests associated with the registered process and the registered computer resource to recognize when the series of operation requests, considered together, has the effect of outputting the registered computer resource to a second computer resource. Klots et al teaches a director keeps track of which resource is handling a request from a process (figure 5, column 6, lines 12-40).

Hunnicutt et al in view of Hipp and Klots et al are analogous art because they are both related to controlling computer resources.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the director in Klots et al with the system in Hunnicutt et al in view of Hipp because fewer system resources are required to manage the system architecture (Klots, column 4, lines 21-25).

Hunnicutt et al in view of Hipp in view of Klots et al teaches the limitations as recited above. It fails to teach monitoring a series of operation requests associated with the registered process and the registered computer resource to recognize when the series of operation requests, considered together, has the effect of outputting the registered computer resource to a second computer resource. Phillips et al teaches monitoring and determining if a request message is able to access a requested file, it is widely known in the art a request may be made in various ways (column 27, lines 39-57).

Hunnicutt et al in view of Hipp in view of Klots et al and Phillips et al are analogous art because they are both related to controlling computer resources.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the monitoring feature in Phillips et al with the system in Hunnicutt et al in view of Hipp in view of Klots et al because maintaining data integrity is provided (Phillips, column 5, lines 56-59).

Claims 57, 58, and 59 disclose the method, apparatus, and medium according to claims 1, 10, and 19 wherein the interception step further comprises intercepting an operation request from the operating system before access to a computer resource. Hipp further teaches intercepting a request from the operating system before access to a computer resource (Figure 3, column 3, line 59 – column 4, line 21).

Claims 7-9, 16-18, and 25-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hunnicutt et al (US Patent #5,889,952) in view of Hipp (US Patent #6,848,106) in view of Klots et al (US Patent #6,920,475) in view of Phillips et al (US

Patent #7,136,903) as applied to claims 1, 10, and 19 above, and further in view of Miller et al (US Patent #5,550,968).

Claims 7, 16, and 25 disclose the method, apparatus, and storage medium according to claims 1, 10, and 19, wherein in the denial step, an access denial error message is returned to the process without any access to the requested computer resource. Hunnicutt et al in view of Hipp in view of Klots et al in view of Phillips et al teaches the limitations of claims 1, 10, and 19, as recited above. It fails to teach returning a denial error message. Miller et al teaches informing the user of an incorrect password (column 9, lines 32-38, figure 5B).

Hunnicutt et al in view of Hipp in view of Klots et al in view of Phillips et al and Miller et al are analogous art because they are both related to providing access control to resources.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the incorrect password technique in Miller et al with the system in Hunnicutt et al in view of Hipp in view of Klots et al in view of Phillips et al because security is provided for individual controls within a window of an interface (Miller et al, column 2, lines 8-10).

Claims 8, 17, and 26 disclose the method, apparatus, and storage medium according to claims 1, 10, and 19, wherein in the denial step, a successful access message is returned to the request source process without any access to the requested computer resource. Hunnicutt et al in view of Hipp in view of Klots et al in view of Phillips et al teaches the limitations of claims 1, 10, and 19 as recited above. It fails to

teach returning a success message without access to the request resource. Miller et al teaches returning a window, as a user would see if access was successful, but with the controls obscured when access is denied (column 9, lines 41-44).

Hunnicutt et al in view of Hipp in view of Klots et al in view of Phillips et al and Miller et al are analogous art because they are both related to providing access control to resources.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the incorrect password technique in Miller et al with the system in Hunnicutt et al in view of Hipp in view of Klots et al in view of Phillips et al because security is provided for individual controls within a window of an interface (Miller et al, column 2, lines 8-10).

Claims 9, 18, and 27 disclose the method according to claims 1, 10, and 19; wherein in the denial step, the operation request is converted into an operation request for a dummy computer resource and transferred to the operating system, and a result from the operating system is returned to the process. Hunnicutt et al in view of Hipp in view of Klots et al in view of Phillips et al teaches the limitations of claims 1, 10, and 19, as recited above. It fails to teach converting the actual request into a request for a dummy resource and returning a result from the operating system. Miller et al teaches a system which returns to a step if the password entry subroutine is ended and displays the window as a user would see if the access was granted but with some fields obscured to the user (column 9, lines 41-44).

Hunnicutt et al in view of Hipp in view of Klots et al in view of Phillips et al and Miller et al are analogous art because they are both related to providing access control to resources.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the incorrect password technique in Miller et al with the system in Hunnicutt et al in view of Hipp in view of Klots et al in view of Phillips et al because security is provided for individual controls within a window of an interface (Miller et al, column 2, lines 8-10).

Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hunnicutt et al (US Patent #5,889,952) in view of Hipp (US Patent #6,848,106) in view of Klots et al (US Patent #6,920,475) in view of Phillips et al (US Patent #7,136,903) as applied to claim 19 above, and further in view of New, JR. et al (US PGPUB #US2003/0028653).

Claim 30 discloses the medium according to claim 19, wherein if it is determined in the determination step that no access right is present, and access is denied in the denial step, an access right is permitted by inputting charging information. Hunnicutt et al in view of Hipp in view of Klots et al in view of Phillips et al teaches the limitations of claim 28 as recited above. It fails to teach granting access rights by charging the requester. New JR. et al teaches billing the user if the requester has insufficient credit (figure 4).

Hunnicutt et al in view of Hipp in view of Klots et al in view of Phillips et al and New JR. et al are analogous art because they are both related to providing access to computer resources.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the traps in New JR. et al with the system in Hunnicutt et al in view of Hipp in view of Klots et al in view of Phillips et al because the system provides added security by preventing unauthorized copies of programs (New JR. et al, paragraph 33, lines 8-13).

Response to Arguments

Applicant's arguments with respect to claims 1, 10, 19, 32-34, and 36-41 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brian J. Gillis whose telephone number is (571)272-7952. The examiner can normally be reached on M-F 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia can be reached on 571-272-3880. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Brian J Gillis
Examiner
Art Unit 2141

/B. J. G./
Examiner, Art Unit 2141
5/20/2008

/Jason D Cardone/
Supervisory Patent Examiner, Art Unit 2145